This presentation may contain simulated phishing attacks.

The trade names/trademarks of third parties used in this presentation are solely for illustrative and educational purposes.

The marks are property of their respective owners and the use or display of the marks does not imply any affiliation with, endorsement by, or association of any kind between such third parties and KnowBe4.

Bad actors don’t care about this and use them anyway to trick you…. 
Emerging Threats, Security Culture

...and How to Protect Your Organization from Cybercriminals

James R. McQuiggan, CISSP
Security Awareness Advocate
James R. McQuiggan, CISSP
Security Awareness Advocate

- Security Awareness Advocate, KnowBe4 Inc.
- Producer, Security Masterminds Podcast
- Professor, Valencia College
- President, (ISC)² Central Florida Chapter
- Board of Trustees, Center for Cyber Safety & Education
- Former Cyber Security Awareness Lead, Siemens Energy
Provider of the world's largest integrated Security Awareness Training and Simulated Phishing platform

Based in Tampa Bay, Florida, founded in 2010

CEO & employees are industry veterans in IT Security.

We help over 50,000 organizations manage the ongoing problem of social engineering

Winner of numerous industry awards

Offices in the USA, UK, Netherlands, Norway, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil
Our mission

To help organizations manage the ongoing problem of social engineering

We do this by

Enabling employees to make smarter security decisions everyday
I Found Gas For Under $2...

James R. McQuiggan
@james_mcquiggan

Taco Bell is the only place you can still get gas for $1.39.
Cybersecurity 101
Reduce your risk
Reduce your exposure
Cybercriminals (Mainly) Gain Access One of Two Ways

Social Engineering

Unpatched Systems
Why hack technology if it’s easier to hack a human?
Humans Are the Biggest Attack Vector
People Are a Critical Layer Within the Fabric of the Security Program
I figured out Forrest Gump’s password

1-Forrest-1
Agenda

- Emerging Threats
- Phishing Issues
- Security Awareness & Culture
Emerging Threats
Current Threat Landscape

- Phishing Attacks
- Business Email Compromise
- Malware / Ransomware
- Password Attacks
Phishing

Opening your front door and letting the cyber criminals into your organization.
Phishing: it is not getting any better

Different types of Attack Vectors

- Spearphishing
- SMSishing
- Vishing
List of Phishing Request Actions

Phishing email arrives via email, web, SMS, social media, voice, collaboration platform etc.

- **Provide Info**
  Including logon credentials, files, W2, info etc.

- **Verification**
  Get a reply to verify account is active

- **Click on URL**
  Always check the link!

- **Call Phone Number**
  To further the social engineering scam (vishing)

- **Open Malware**
  Open or Download Malicious Content

- **Pay Something**
  Fines, Taxes, Bills, Subscriptions

- **Access to System**
  Provide Access to legitimate system or feature

- **Added Communication**
  To continue the fraud
Business Email Compromise (BEC)

Wire Transfer Fraud

W2 Fraud

Gift card Fraud
Most Interesting Phishing Techniques: iTunes Gift Cards

From: John Carpenter <officeexec.mails@inbox.lv>
To: Emily Walker <ewalker@distracted.com>

Hi Emily, Let me know when you are available. There is something I need you to do.

I am going into a meeting now with limited phone calls, so just reply to my email.

From: Emily Walker <ewalker@distracted.com>
To: John Carpenter <officeexec.mails@inbox.lv>

Did you intend to send this to me?

From: John Carpenter <officeexec.mails@inbox.lv>
To: Emily Walker <ewalker@distracted.com>

Yes Emily, can you get this done ASAP? I need some couple of gift cards.

There are some listed clients we are presenting the gift cards. How quickly can you arrange these gift cards because I need to send them out in less than an hour. I would provide you with the type of gift cards and amount of each.

From: Emily Walker <ewalker@distracted.com>
To: John Carpenter <officeexec.mails@inbox.lv>

Can do now. I’ll put on my credit card. Send me the following:

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
<th>Amount</th>
</tr>
</thead>
</table>

KnowBe4: Human error Conquered
Most Interesting Phishing Techniques: iTunes Gift Cards

From: John Carpenter <officeexec.mails@inbox.lv>
To: Emily Walker <ewalker@distracted.com>

The type of card I need is Apple iTunes gift cards. $100 denomination, I need $100 X 20 cards. You might not be able to get all in one store, you can get them from different stores. When you get the cards, Scratch out the back to reveal the card codes, and email me the codes. How soon can you get that done? Its Urgent.

From: Emily Walker <ewalker@distracted.com>
To: John Carpenter <officeexec.mails@inbox.lv>

On my way to store now. What time do you need them by?

From: John Carpenter <officeexec.mails@inbox.lv>
To: Emily Walker <ewalker@distracted.com>

As soon as you can. I will await codes

From: Emily Walker <ewalker@distracted.com>
To: John Carpenter <officeexec.mails@inbox.lv>

Just texted you the first 11 codes. Heading to another store now. 5 and 6 limit per store.
Most Interesting Phishing Techniques: iTunes Gift Cards

From: John Carpenter
<officeexec.mails@inbox.lv>
To: Emily Walker <ewalker@distracted.com>

Email them to me
Ransomware Stats – Comparitech (2021)

- 576 US organizations hit / ~7% drop from 2020
- More targeted, more devasting
- 34.1 million records stolen = $159.4 billion in downtime
- Average ransom - $5.8 million
  - $2 million in 2020
- Average ransom payment was $7.9 million
  - ~$1 million in 2020
- ~$3.4 billion last year in total ransom demands
- $1.3 billion in bounty for hackers. (<30%)
- 22 days average of lost time
- The top 5 states affected by ransomware attacks:
  - California, Massachusetts, Texas, New York, Illinois

https://www.comparitech.com/blog/information-security/us-ransomware-attacks-cost/
What Ransomware Looks Like Now

Ransomware Workflow

1. Victim tricked into executing “stager” trojan horse program, modifies host system
2. After executing, it immediately downloads updates and additional malware & instructions from C&C servers
3. Updates itself to keep ahead of AV/EDR detection, new payloads, spreads
4. Collects as many passwords as it can
5. Notifies C&C/hacker about new intrusion
6. Dwells (sometimes up to 8 to 12 months)
7. Hackers come in, assess and analyze target
8. Steal whatever they want
9. Launch encryption and ask for ransom
Ransomware Attack - Video
Ransomware Is a Data Breach

- Criminal hackers infiltrate the network
- Install Trojans / other malware
- Delete backups
- Steal data before encryption
- Double / Triple Extortion
- Leak Data, Intellectual Property
- Public Shaming / Threatening Victim’s Customers
- Release data if LEO are contacted
Password Attacks

Akamai: We Saw 61 Billion Credential Stuffing Attacks in 18 Months

2.2 Billion Accounts Found In Biggest Ever Data Dump -- How To Check If You're A Victim

Davey Winder | Senior Contributor @Cybersecurity
I report and analyse breaking cybersecurity and privacy stories

KnowBe4
Human error. Conquered.
Real World Stories - City of Oldsmar Water Treatment Attack

- Infiltrated to change settings
- Access to legacy SCADA systems
- No Firewall
- Concerns about remote access
- No separation of equipment
- Running Windows 7
- **THE BIG ISSUE:**
- Password used was never changed after it was a previous data breach collection
Real World Stories – Sticky Notes

- Post-it Notes
- Posted on Social Media
- NoMar5456 – Gmail
Stolen & Weak Passwords

Most data breaches involve weak, default, or stolen passwords

- 81% of breaches are caused by credential theft\(^4\)
- 73% of passwords are duplicates\(^5\)
- 50% of employees use apps that aren’t approved by the enterprise\(^6\)

\(^4\) 2018 Verizon Data Breach report, aka.ms/dbir2018
\(^5\) 2016 Telesign Consumer account security report, aka.ms/tcasr2016
\(^6\) 2019 Igloo State of the Digital Workplace report, aka.ms/isdwr2019
Would you consider these weak passwords and difficult to hack or figure out?
### Current Hacked Passwords

- No brute force
- Using rainbow tables with 8 billion different passwords
- Passwords that have been stolen, collected or cracked
- Took about 2 days
- Some meet requirements but were crackable
- Other ones included:
  - Sh3rl0ck123456789
  - Qwertyuiop1234$%
  - Manchester101497!
  - Salesrecruiter2022!
  - Ilovelucyverymuch122

<table>
<thead>
<tr>
<th>#</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>D0gschasecats245</td>
</tr>
<tr>
<td>2</td>
<td>Version1234567890</td>
</tr>
<tr>
<td>3</td>
<td>Love77hate!!!!!!!</td>
</tr>
<tr>
<td>4</td>
<td>best is yet to come</td>
</tr>
<tr>
<td>5</td>
<td>Royalenfield@123</td>
</tr>
<tr>
<td>6</td>
<td>Peaceandlove1999!</td>
</tr>
<tr>
<td>7</td>
<td>Bakerboysdist6!!!</td>
</tr>
<tr>
<td>8</td>
<td>Theorderofthewhitelotus</td>
</tr>
<tr>
<td>9</td>
<td>iloveAmsterdam2022!</td>
</tr>
<tr>
<td>10</td>
<td>ILoveFriedChicken1314</td>
</tr>
<tr>
<td>11</td>
<td>Persillehaven42!</td>
</tr>
<tr>
<td>12</td>
<td>Enterprise Sales</td>
</tr>
<tr>
<td>13</td>
<td>BobbaFett123456!</td>
</tr>
<tr>
<td>14</td>
<td>RainRainGoAway!!2</td>
</tr>
<tr>
<td>15</td>
<td>Theblacklegion!88</td>
</tr>
<tr>
<td>16</td>
<td>slaughterhouse45!</td>
</tr>
<tr>
<td>17</td>
<td>Creativelam2022!</td>
</tr>
<tr>
<td>18</td>
<td>Velvetditch2020!</td>
</tr>
<tr>
<td>19</td>
<td>Bogeybogeybogey13!</td>
</tr>
<tr>
<td>20</td>
<td>Harrison30149824</td>
</tr>
<tr>
<td>21</td>
<td>123Iwantthatway!</td>
</tr>
<tr>
<td>22</td>
<td>Wizkhalifa.17410</td>
</tr>
<tr>
<td>23</td>
<td>Dingowashisname0!</td>
</tr>
<tr>
<td>24</td>
<td>Raidernation2022!</td>
</tr>
</tbody>
</table>
Why doesn’t Superman fight cybercrime?

He’s afraid of Krypto-currency.
Phishing Issues

Stop Phishing

Attacks
Why do we fall victim to phishing?
Understanding the root of deception

Our brains’ job to filter, interpret, & present ‘reality’
WHAT I IF TOLD YOU
YOU READ THE TOP LINE WRONG.
Perception vs. Reality - Reading

The phaonmneal pweor of the hmuan mnid, aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttae in waht oredr the ltteers in a wrod are, the olny iprmoatnt tihng is taht the frist and lsat ltteer be in the rghit pclae. The rset can be a taotl mses and you can sitll raed it wouthit a porbelm.
Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe. Amzanig huh?
And I awlyas tghuhot slpeing was ipmorantt!
Let’s have some fun for a moment
Pick a Card!
Is it gone now?
How Did We Identify and Remove Your Card?

Here’s what we started with:

And here’s what we ended with:
Thinking, Fast & Slow (Daniel Kahneman)

**System 1 (Fast Thinking)**
- Continuously scans our environment.
- Fast but error-prone
- Works automatically & effortlessly via shortcuts, impulses and intuition.

**System 2 (Slow Thinking)**
- Used for specific problems, only if necessary
- Takes effort to analyze, reason, solve complex problems, exercise self-control
- Slow but reliable

System 1 Thinking Example

2 + 2 = 4
System 2 Thinking Example

Solve for $x$:

$$\frac{5327}{86} = x$$
Social Engineering

Are You Being Manipulated?
-- understand the lures --

Greed  Curiosity  Self Interest
Urgency  Fear  Helpfulness
Who’s At Risk?

- New, seasonal or temporary employees
- Senior people (managers, directors, privileged users)
- Maintenance staff (cleaners, security guards, vendors)
- People who are active or chatty on social media.
- HR departments
- Everyone is at risk.
Victimless Thinking

Sophisticated Cybercriminals

Critical Account Weakness

Password Re-use

Latest Scam Unawareness

Silver Bullet Protections
Security Awareness & Culture
Security Awareness & Training

**Baseline Testing**
We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

**Train Your Users**
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

**Phish Your Users**
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

**See the Results**
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!
## Phase Three

Phishing Security Test Results After One Year-Plus of Ongoing Training

<table>
<thead>
<tr>
<th>Organization Size</th>
<th>12-Month PPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-249</td>
<td>3.8%</td>
</tr>
<tr>
<td>250-999</td>
<td>5%</td>
</tr>
<tr>
<td>1000+</td>
<td>5.8%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Industry</th>
<th>1-249 Employees</th>
<th>250-999 Employees</th>
<th>1000+ Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking</td>
<td>2.6%</td>
<td>3.3%</td>
<td>3.4%</td>
</tr>
<tr>
<td>Business Services</td>
<td>3.8%</td>
<td>5%</td>
<td>6%</td>
</tr>
<tr>
<td>Construction</td>
<td>4.1%</td>
<td>4.8%</td>
<td>4.6%</td>
</tr>
<tr>
<td>Consulting</td>
<td>3.8%</td>
<td>4.8%</td>
<td>4.9%</td>
</tr>
<tr>
<td>Consumer Services</td>
<td>4.7%</td>
<td>4.7%</td>
<td>3.3%</td>
</tr>
<tr>
<td>Education</td>
<td>4.1%</td>
<td>5.4%</td>
<td>6.5%</td>
</tr>
<tr>
<td>Energy &amp; Utilities</td>
<td>3.4%</td>
<td>5%</td>
<td>3.6%</td>
</tr>
<tr>
<td>Financial Services</td>
<td>3.7%</td>
<td>4.9%</td>
<td>5.5%</td>
</tr>
<tr>
<td><strong>Government</strong></td>
<td><strong>3.9%</strong></td>
<td><strong>3.9%</strong></td>
<td><strong>7.1%</strong></td>
</tr>
<tr>
<td>Healthcare &amp; Pharmaceuticals</td>
<td>4.1%</td>
<td>5.1%</td>
<td>5.9%</td>
</tr>
<tr>
<td>Hospitality</td>
<td>4.4%</td>
<td>5.6%</td>
<td>1.3%</td>
</tr>
<tr>
<td>Insurance</td>
<td>3.3%</td>
<td>4%</td>
<td>5.3%</td>
</tr>
<tr>
<td>Legal</td>
<td>4.1%</td>
<td>5.2%</td>
<td>5.6%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>3.3%</td>
<td>5.3%</td>
<td>6.2%</td>
</tr>
<tr>
<td>Not-For-Profit</td>
<td>4.1%</td>
<td>4.9%</td>
<td>4.5%</td>
</tr>
<tr>
<td>Other</td>
<td>3.2%</td>
<td>4%</td>
<td>6.2%</td>
</tr>
<tr>
<td>Retail &amp; Wholesale</td>
<td>3.6%</td>
<td>5.3%</td>
<td>4.7%</td>
</tr>
<tr>
<td>Technology</td>
<td>4.7%</td>
<td>5.9%</td>
<td>7.2%</td>
</tr>
<tr>
<td>Transportation</td>
<td>4.1%</td>
<td>9.6%</td>
<td>4.5%</td>
</tr>
</tbody>
</table>
Phishing Example

From: Zoom <noreply@meet-zoom.us>
Reply-To: Zoom <noreply@meet-zoom.us>
Subject: You missed a Zoom meeting

You missed a meeting

Date: [[current_date_0]]
Duration: 29:50

You did not attend today's meeting. For more information on the meeting or to reschedule, click the link below.

See Details

To listen to this message, you can open the attachment or use any Zoom Applications to have instant access to all your messages.
Stages of Post Phishing / Social Engineering Attack

Shock

Denial

Anger

Acceptance
It’s a Teaching Moment
Oops...

Chicago Tribune (09/20)

GoDaddy (12/20)

West Midlands (5/21)

OHSU (04/22)
4 Questions to Ask Your Email

Email
Is the email unexpected?

Sender
Is this person a stranger? #StrangerDanger

Action
1. Are they asking me to do something immediately or quickly?
2. Does the action seem strange or unusual?

Verify
Attempt to use a second connection to verify the email

YES?
Social Engineering Red Flags

FROM
- I don't recognize the sender's email address as someone I ordinarily communicate with.
- This email is from someone outside my organization and it's not related to my job responsibilities.
- This email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- Is the sender's email address from a suspicious domain (like microsoft-support.com)?
- I don't know the sender personally and they were not vouched for by someone I trust.
- I don't have a business relationship nor any past communications with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven't communicated with recently.

DATE
- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?

SUBJECT
- Did I get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?

TO
- I was cc'd on an email sent to one or more people, but I don't personally know the other people it was sent to.
- I received an email that was also sent to an unusual mix of people.
- For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS
- I hover my mouse over a hyperlink that's displayed in the email message, but the link to address is for a different website. (This is a big red flag.)
- I received an email that only has long hyperlinks with no further information, and the rest of the email is completely blank.
- I received an email with a hyperlink that is a misspelling of a known web site. For instance, www.bankofamerica.com — the "m" is really two characters — "r" and "n."

ATTACHMENTS
- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly dangerous file type. The only file type that is always safe to click on is a .txt file.

CONTENT
- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click a link or open an attachment that seems odd or illogical?
- Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?
Check for Rogue URLs

- Check your links!
- Look for transposed letters or used other symbols in the websites
  - Micorsoft.com (transposed)
  - G00GLE.com (similar letters)
  - Bankofarnerica.com (combined r n -> m)
  - wikipedia.org vs wikipedia.org (homograph)
Why Is Getting the Desired Behaviors So Difficult?

BJ Fogg
@bjfogg

3 truths about human nature: We're lazy, social, and creatures of habit. Design products for this reality.
10:59 AM - 31 Mar 2011
Behavior happens when three things come together at the same time:

**Motivation, Ability, and a Prompt** to do the behavior…

http://behaviormodel.org

**BJ Fogg** is the father of a field now referred as “Behavior Design.”
A Cybersecurity Example – Phishing Email

**Motivation**
- Make sure it’s not a phishing link
- Not have to do remedial training
- Protect the organization

**Ability**
- Know how to find the link
- Understand the make up of a URL

**Prompt**
- The email may appear to be strange, not expected
- They had training to know about phishing emails
- The LinkedIn email is to your work, not your personal email
Nudge your audience toward the behavior

Nudge Them in the Right Direction

Your password change portal is a great place to insert a nudge:

• Strength Meters
• Videos on how to create & remember strong passwords
• Elective LMS modules
• etc.
Password Vault

It reduces your risk because it can:

• Store credential information
• Generate the strong passwords
• Alert you of compromised accounts
• Keep the passwords unique
• If possible, unique usernames too
• Store the security question responses
  • With social media it’s easier to discover the answers
  • Consider different / wrong answers
• Free vs Paid Options
Why Don’t People Use Password Managers?

• Need to insert all passwords
  • Takes too long
  • Browsers
  • Notepaper
  • Word/Excel
• Trust Issues with developer
  • Giving up too much data
• Single Point of Failure
  • Lose master password
Ways to Protect / Check Your Email

- Have I been Pwned?
- [https://haveibeenpwned.com](https://haveibeenpwned.com)
- Alerts you data breaches
- If it happens, change your password even if it’s got MFA
- Change the password on other accounts that use the same password
Use Multi Factor Authentication

SMS (Okay)
- It’s okay – not the best
- Unfortunately this is commonly used

Application (Better)
- Code Generated in App
- Make sure you can back them up

Hardware (best)
- Uses a hardware token, like a Yubikey or your smartphone
- Can be inconvenient when forgotten or damaged
Mitnick MitM PayPal Attack - Video
Example MitM MFA Hack

Network Session Hijacking

1. Attacker socially engineers victim to visit a rogue and usually look-alike web site
   • Proxies input to real web site
2. Prompts victim to enter MFA credentials
3. Victim enters credentials, which attacker relays to real web site
4. Attacker intercepts victim’s resulting access control token
5. Attacker logs into real site, and drops legitimate user
6. Takes control over user’s account
7. Changes anything user could use to take back control

https://blog.knowbe4.com/heads-up-new-exploit-hacks-linkedIn-2-factor-auth.-see-this-kevin-mitnick-video
Password Use Recommendations

- **MFA**: If possible, use MFA
- **Unique Passwords**: Complex passwords (No reuse)
- **Password Manager**: It creates long, strong, unique passwords for you
- **Create your own?**: Better
  - At least 12 characters, complex
  - 16+ character / passphrase
Most Secure Woman?

MFA

Emma Faye

Multifactor Authentication
Security Awareness Has Evolved

- **In-House**: The “Do-It-Yourself” era of in-house, ineffective offerings

- **Basic Content Vendors**: Content and Newsletter vendors offering stale answers to a fresh problem

- **Phishing Simulation**: The start of the first behavior management awareness programs

- **Meaningful Metrics**: Ability to report relevant analytics pertaining to behavior change, human risk, and engagement

- **Security Culture**: The rise of security culture management

  - Awareness permeates throughout the entire organization
  - Collectively mitigates the risk of the human element
  - Converges with the maturation of the CISO role

- **The rise of Ransomware created a market inflection point**

- **Statistics interesting to executive teams, boards, regulators, auditors**
Organizations believe security culture is important for success.
However, culture remains highly undefined

- **29%** Compliance to security policies
- **24%** Awareness and understanding of security issues
- **22%** Security is everyone’s responsibility
- **14%** Security advocacy and support
- **12%** Security embedded in the organization

*Base: 784 global enterprise security or risk managers that influence their organizations security policies*

*Source: A commissioned study conducted by Forrester Consulting on behalf of KnowBe4, December 2019*
Security culture is defined as the ideas, customs, and social behaviors that impact the security of your organization.
Consider Your Security Culture Posture?

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Compliance</td>
<td>Security Awareness Foundation</td>
<td>Programmatic Security Awareness &amp; Behavior</td>
<td>Security Behavior Management</td>
<td>Sustainable Security Culture</td>
</tr>
</tbody>
</table>

The dashed red line represents breach likelihood and relative cost remediation.
The solid blue line represents awareness/culture maturity gains at each stage of the model.

Source: KnowBe4
Strong Security Culture Leads To 52x Less Credential Sharing

As organizations improve their security culture, the risky behaviors of their employees are reduced.
SAFETY FIRST

DAYS SINCE LAST INJURY

365
SAFETY FIRST

DAYS SINCE
LAST CYBER INCIDENT

???
Think Like an Attacker, Plan Like a Marketer
Final Thoughts
Organizations should care about their ROI when it comes to cybersecurity

Reduction of Investment
Significant Underinvestment in Security Awareness

Worldwide IT Security Products Spend¹

<table>
<thead>
<tr>
<th>Category</th>
<th>Spend ($Bn)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>47%</td>
</tr>
<tr>
<td>Endpoint</td>
<td>22%</td>
</tr>
<tr>
<td>Web</td>
<td>14%</td>
</tr>
<tr>
<td>Identity</td>
<td>14%</td>
</tr>
<tr>
<td>Human</td>
<td>&lt;3%</td>
</tr>
</tbody>
</table>

Source: IDC

¹ Breakdown of worldwide IT security products spend as of 2019.
# 15 Cybersecurity Best Practices

<table>
<thead>
<tr>
<th>Security Awareness / Security Culture</th>
<th>Adopt a Framework – CSFW, HIPAA, ISO, CIS</th>
<th>Identify your systems / data AKA Asset Inventory</th>
<th>Backup Your Data</th>
<th>Implement MFA for applications, sensitive systems, logins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patching / Patch Management</td>
<td>Least User Privilege (Account Management)</td>
<td>Harden Software / Hardware</td>
<td>Malware Defenses</td>
<td>Cyber Incident / Response (Disaster Recovery)</td>
</tr>
</tbody>
</table>
CISA Tips for Shields Up

• Internet Facing Systems
  • Be aware of all external facing systems
  • Make sure they’re patched up to date on all security updates
  • Implement MFA on authorization systems from the outside – Preferably with an App
  • Review all Remote Access connections

• Backups – check them and test them

• Technology
  • Protect against DDoS attacks
  • Restrict firewall communication inbound for only necessary traffic
  • Monitor Outbound traffic for anomalies

• Vulnerability Management – Review CISA vulnerabilities catalog

• Endpoint Solutions – EDR

• Network Segmentation
  • Trusted Zones for sensitive systems

• Least Privilege Use

• Human Detection & Response – HDR
What it’s like for your IT Team
What it feels like somedays
This goes way beyond awareness or coercing secure behaviors. It's about making workers value security ...where they proactively participate in taking steps that reduce risk.

-Perry Carpenter
The podcast that brings you the very best in all things, cybersecurity, taking an in-depth look at the most pressing issues and trends across the industry.
YouTube: James McQuiggan and Dad Jokes
https://www.youtube.com/channel/UCxgX_WNpq-ovODjdIDco4zw

Know more about KnowBe4.
James R. McQuiggan, CISSP
jmcquiggan@knowbe4.com
@james_mcquiggan
Thank you for your attention

Questions?

For more information visit blog.knowbe4.com

Know more about KnowBe4.
James R. McQuiggan, CISSP
jmcquiggan@knowbe4.com
@james_mcquiggan
Resources

• Contact Info
  • LinkedIn: https://www.linkedin.com/in/jmcquiggan/
  • Twitter: https://twitter.com/James_McQuiggan
  • Email: jmcquiggan@knowbe4.com
  • YouTube: https://www.youtube.com/channel/UCxgX_WNpq-ovODjdIDco4zw

• KnowBe4
  • Blog – https://blog.knowbe4.com
  • Rogue URLs PDF - https://www.knowbe4.com/hubfs/Red%20Flags%20of%20Rogue%20URLs%20(3).pdf
  • KnowBe4 Home Course Training (password: homecourse) https://www.knowbe4.com/homecourse
  • Ransomware Hostage Rescue Manual: https://www.knowbe4.com/ransomware
  • KnowBe4 Compliance Manager - kcmgrc.knowbe4.com
Ransomware, Phishing & Culture

For more information visit blog.knowbe4.com